Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/082,600	GRAWROCK, DAVID W.
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>09 February 2006</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-44</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) <u>27-34 and 41-44</u> is/are allowed.

6)☒ Claim(s) <u>1-6,9-21,35 and 40</u> is/are rejected.

7)☒ Claim(s) <u>7,8,22-26 and 36-39</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>22 February 2002</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>13 documents</u>.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

Response to Amendment

1.   This office action is responsive to Applicant's amendment received on 2/9/2006.

Claims 1-44 are pending.

Information Disclosure Statement

2.   The information disclosure statement (IDS) documents submitted as of the date

of this office action have been considered.

Response to Arguments

3.   Applicant's arguments filed 2/9/2006 have been fully considered but they are not

persuasive.

Regarding claims 1-6 and 9-14, Applicant argues that Knapton does not disclose

1) requesting tokens to unseal portions of a multi-token sealed object and 2) decrypting

the component password to allow use of the component (Remarks, page 2-4).

Examiner responds that Knapton discloses, " ... the controller security control creates

an encrypted application key, using at least a portion of the application license number

and a secret encryption key as input data. In one embodiment, the application key is

encrypted according to the well-known Data Encryption Standard (DES) technique,

although other encryption techniques may also be employed. The secret encryption

key comprises a predetermined data value known by the controller security control

operation of the controller computer system, but it is not known by any end user. In

embodiments using the DES technique or other two key encryption processes, the

secret encryption key is a private key. In this manner, in this particular embodiment the encrypted application key is associated with the specific copy of the application program that the requesting end user has previously been authorized to use. Of course, the invention is not restricted in scope in this respect. ... the controller security control operation creates an encrypted component key, using a unique identifier for the requested component and the secret encryption key as input data. As with generation of the application key, in one embodiment, the component key may be encrypted according to the well-known DES technique, although other encryption techniques may also be employed. In one embodiment, if the requested component is an ActiveX control, a global unique identifier (GUID) for the component may be used as the identifier. In this manner, the encrypted component key is uniquely associated with a specific copy of the requested component. Next, at block 208, the controller security control creates an encrypted component password, by combining the encrypted application key and the encrypted component key and encrypting the resulting combination. ... "(i.e., application program functions as the first token while the component works as the second token)(col. 5, lines 10-67). Kanpton also inherently discloses the decryption of the component password when the application program compares the generated component password with the stored component password and allows use of the component if there is a match (i.e., please note that decrypting the data encryption key using the key encryption key is well-known in the art)(col. 7, lines 39-51).

Regarding cliams 15-21, 35, and 40, Applicant argues that Knapton does not disclose requesting tokens to seal portions of a multi-token sealed object to environment criteria (Remarks, page 4-6).

Examiner responds that Knapton discloses, " ... a component functions only with the application program that has the licence number that was provided when the component was licenced. If another copy of the application program attempts to access the component (e.g., the component was copied to another computer system having an application program with a different license number), the component will not be snapped in. ..." (col. 3, lines 8-29).

4.   Regarding claims 1-6, 9-21, 35, and 40, Examiner respectfully maintains the 35 U.S.C. 102 (b) rejection communicated on 11/7/2005 as follows:

Allowable Subject Matter

Claims 7-8, 22-26, and 36-39 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6, 9-21, 35, and 40 are rejected under 35 U.S.C. 102(b) as being

anticipated by Knapton, III, (U.S. Patent No. 6,363,486 and Knapton hereinafter).

Regarding claims 1-2, 10-11, and 15, Knapton discloses a method comprising:

requesting a first token (i.e., identifier of the appliation program) to unseal a

sealed first portion of a multi-token sealed object to obtain a first portion of the multi-

token sealed object, requesting a second token (i.e., identifier of the component) to

unseal a sealed second portion of a multi-token sealed object to obtain a second portion

of the multi-token sealed object, and using the first portion and the second portion to

obtain an object from the multi-token sealed object (i.e., generating a first password

from the application program identifier and a second password form the identifier of the

component and allowing use of the component with the application program on the

computer system if the first and the second passowrd match)(Col. 5, lines 10-67 and

Col. 6, lines 1-67).

Regarding claims 4-5, Knapton discloses further comprising:

generating a key from the first portion and the second portion of the multi-token

sealed object, and obtaining the object of the multi-token sealed object by using the

generated key and an asymmetric cryptographic algorithm to decrypt an encrypted

object of the multi-token sealed object (Col. 6, lines 1-40).

Regarding claims 3, 6, and 9, Knapton discloses further comprising:

receiving a first key in response to the first token unsealing the sealed first

portion (i.e., first password) only if the first token generated the sealed first portion,

receiving a second key in response to the second token unsealing the second portion

(i.e., second password) only if the second token generated the sealed second portion,

generating a third key from the first key and the second key, and obtaining the object of

the multi-token sealed by using the third key to decrypt an encrypted object of the multi-

token sealed object (i.e., generating a first password from the application program

identifier and a second password form the identifier of the component and allowing use

of the component with the application program on the computer system if the first and

the second passowrd match)(Col. 5, lines 10-67 and Col. 6, lines 1-67).

Regarding claims 12 and 16, Knapton discloses further comprising:

encrypting an object using a symmetric cryptographic algorithm and a key to

obtain an encrypted object, and receiving a sealed encrypted object in response to the

first token sealing the first portion that comprises the encrypted object, receiving a

sealed key in response to the second token sealing the second portion that comprises

the key (Col. 6, lines 1-40).

Regarding claim 17, Knapton discloses further comprising:

encrypting the object using an asymmetric cryptographic algorithm and an

encryption key of an asymmetric key pair to obtain an encrypted object, receiving a

sealed encrypted object in response to the first token sealing the first portion that

comprises the encrypted object, receiving a sealed decryption key in response to the

second token sealing the second portion that comprises a decryption key of the

asymmetric key pair (Col. 6, lines 1-40).

Regarding claims 13-14 and 18, Knapton discloses further comprising:

receiving a sealed first portion encrypted by the first token using a first key of the

first token, the sealed first portion comprising the first key, a first seal record comprising

one or more metrics specified by the first environment criteria (i.e., identifier of the

appliation program), and a first digest value that attests to the integrity of the first key

and the first seal record (i.e., generating a first password from the application program

identifier), and receiving a sealed second portion encrypted by the second token using a

second key of the second token, the sealed second portion comprising the second key,

a second seal record comprising one or more metrics specified by the second

environment criteria (i.e., identifier of the component), and a second digest value that

attests to the integrity of the second key and the second seal record (i.e., generating a

second password form the identifier of the component)(Col. 5, lines 10-67 and Col. 6,

lines 1-67).

Regarding claim 19, Knapton discloses wherein the first seal record comprises a

unique first identifier for the first token, and the second seal record comprises a unique

second identifier for the second token (Col. 2, lines 24-44).

Regarding claim 20, Knapton discloses further comprising:

encrypting the object using key that was generated based upon a first key and a

second key, receiving a sealed first key in response to the first token sealing the first

portion that comprises the first key, receiving a sealed second key in response to the

second token sealing the second portion that comprises the second key (Col. 2, lines

24-44).

Regarding claim 35, Knapton discloses a machine readable medium comprising

a plurality of instructions that, in response to being executed, result in a computing

device sealing a first portion of a multi-token sealed object to first environment criteria

using a first public key of a first token to obtain a sealed first portion, and sealing a

second portion of the multi-token sealed object to second environment criteria using a

second public key of a second token to obtain a sealed second portion (i.e., Application

program 12 also comprises application security control function 22, which operates to

ensure that in this embodiment only licensed components are used with the application

program)(Col. 2, lines 24-44 and Col. 3, lines 7-59).

Conclusion

5.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-

3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for

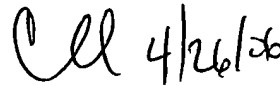the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

A.S.

Patent Examiner
Group 2131
April 26, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER